Kriminalitätsbekämpfung im Dark Net: neue Ermittlungsansätze statt Verbote

Schulze, Matthias

Veröffentlichungsversion / Published Version
Arbeitspapier / working paper

Zur Verfügung gestellt in Kooperation mit / provided in cooperation with:
Stiftung Wissenschaft und Politik (SWP)

Empfohlene Zitierung / Suggested Citation:
Schulze, M. (2019). *Kriminalitätsbekämpfung im Dark Net: neue Ermittlungsansätze statt Verbote.* (SWP-Aktuell, 28/2019). Berlin: Stiftung Wissenschaft und Politik -SWP- Deutsches Institut für Internationale Politik und Sicherheit. https://doi.org/10.18449/2019A28

SWP

SWP-Aktuell

NR. 28 APRIL 2019

Kriminalitätsbekämpfung im Dark Net

Neue Ermittlungsansätze statt Verbote

Matthias Schulze

Gegenwärtig werden wieder Forderungen nach einem Verbot illegaler Bereiche im Internet – sogenannter Dark Nets – laut. Im Entwurf des Bundesinnenministeriums für das neue IT-Sicherheitsgesetz soll das »Zugänglichmachen von Leistungen zur Begehung von Straftaten« über internetbasierte Dienste unter Strafe gestellt werden. In der öffentlichen Wahrnehmung dominieren insbesondere die negativen Aspekte des Dark Nets: illegaler Waffen- und Drogenhandel, Cyber-Kriminalität und Kinderpornografie. Neuere Daten zeigen jedoch, dass die Bedrohungen, die vom Dark Net ausgehen, weitaus geringer sind als häufig angenommen. Daher ist zu fragen, ob ein Verbot dieser Technologie sinnvoll, ohne negative Kollateraleffekte umsetzbar und zudem verhältnismäßig ist. Statt das Dark Net als solches verbieten zu wollen, sollte der Fokus darauf gerichtet werden, in neuen Ermittlungstechniken zu schulen und die internationale Kooperation bei der Strafverfolgung zu intensivieren. Dies wäre eine nachhaltige Lösung, da diese Fähigkeiten auch im Kampf gegen das weitaus größere Problem – Cyber-Kriminalität im regulären Internet – von Nutzen wären.

Im politischen Diskurs ist oft nicht klar, was unter dem Dark Net verstanden wird. Das Internet ist ein Netzwerk, das Milliarden von Geräten mittels kleinerer Netzwerke (LAN, WLAN, WAN, Mobilfunk) in eine große Infrastruktur integriert. Es werden drei Ebenen unterschieden: die Ebene der *Anwendungen* des Internets (etwa das World Wide Web bzw. WWW, Datenbanken oder Apps), die *Protokoll-* bzw. *Netzwerkebene* der Datenübertragung und die Ebene der *Hardware* (Router, Glasfaserleitungen). Ein Merkmal des Internets ist, dass es keinen zentralen Wachturm gibt, der das gesamte Netzwerk überblicken kann. Folglich gibt es sichtbare und unsichtbare Bereiche, sowohl auf der Protokoll- als auch auf der Anwendungsebene.

Zu den *sichtbaren Bereichen* zählt in erster Linie das *World Wide Web*. Das WWW in Form von Websites ist lediglich der Bereich, der über den Browser sichtbar ist. Man schätzt, dass es circa 1,6 Milliarden Websites im WWW gibt (davon wird die überwiegende Mehrheit nicht mehr aktualisiert).

Unsichtbare Teile des Internets, das sogenannte *Deep Net*, sind zum Beispiel Datenbanken und Apps, die nicht öffentlich oder nur eingeschränkt zugänglich sind. Dazu gehören Firmen- oder Regierungsnetzwerke. Es wird vermutet, dass das gesamte Internet aus circa 40 000 Deep Nets besteht.

Stiftung Wissenschaft und Politik
Deutsches Institut für Internationale Politik und Sicherheit

Das *Deep Web* wiederum wird häufig als jener Bereich des WWW bezeichnet, der nicht von Suchmaschinen indiziert wird. Die Services von Facebook, Twitter und Snapchat sind Teil des Deep Webs, da sie nur durch eine Applikation bzw. passwortgeschützte Programminterfaces aufgerufen werden können. Seiten, die nicht von Suchmaschinen erfasst werden, sind Teil des Deep Web. Das sind sozusagen Orte des WWW, die zwar existieren, aber auf keiner Karte auftauchen.

Zu guter Letzt gibt es noch verschiedene *Dark Networks* als Teilbereich des Internets. Diese werden ebenfalls nicht von Suchmaschinen indiziert und basieren auf eigenen Übertragungsprotokollen (etwa dem Onion Service Protocol). Dieses Protokoll verschlüsselt die Kommunikation und leitet sie mehrfach über sogenannte Relay-Server um, so dass Inhalte und IP-Adressen für Außenstehende unsichtbar werden. Auch innerhalb des Dark Nets gibt es wieder eine Ebene der Netzwerkkommunikation, das *Tor Netzwerk (The Onion Routing)*, und eine Ebene der Anwendungen, in Form von *Tor Hidden Services (HS)* oder anderen Anwendungen wie *OnionShare* (ein anonymer Cloud-Speicher). Tor Hidden Services sind oft Websites, können aber auch Steuerungsserver zur Kontrolle von Bot-Netzen sein. Die Summe der Seiten bildet ein *Dark Web*. Viele der darin enthaltenen HS-Websites können nur von denjenigen besucht werden, die die Onion-Adresse des HS kennen. HS sind ein optionales Feature des Tor-Netzwerks, das es Website-Besuchern und Website-Servern ermöglicht, sich anonym gegenüberzustehen. Technisch funktioniert dies wie ein sogenannter »toter Briefkasten«: Website-Betreiber speisen eine Information ein, die dann später von einem Website-Besucher anonym aufgesammelt wird.

Verglichen mit dem WWW machen HS-Websites nur einen verschwindend geringen Anteil aller Websites aus. Es gibt circa 110 000 HS. HS werden von nur 1 — 3 Prozent der regelmäßig aktiven 2 Millionen Tor-Nutzer überhaupt aufgerufen. Aufgrund der Anonymisierungsfunktion des Tor-Netzwerks sind genaue Metriken allerdings kaum zu bekommen, weshalb hier mit Ungenauigkeiten gerechnet werden muss. HS machen schätzungsweise zwischen 3 und 6 Prozent des Datenverkehrs des Tor-Netzwerks aus. Tor-Nutzer sind also nicht automatisch Dark-Web-Nutzer.

Die folgende Grafik veranschaulicht die hierarchischen Beziehungen zwischen den verschiedenen Teilnetzwerken:

Differenzierung von Netzwerk- und Web-Protokollen

Anwendungs-ebene	**Protokoll-Ebene**	
	Internet (TCP/IP)	40 — 50 Mrd. Geräte in 40 000 Netzwerken
World Wide Web	HTTP	ca. 1,6 Mrd. Websites
Deep Web	**Deep Net** (802.11-WLAN, Ethernet)	
Dark Web (Tor Hidden Services, Freenet etc., Onion Sharing)	**Dark Nets** (z.B. Onion Service Protocol, I2P und weitere)	ca. 2 Mio. Tor-Nutzer; ca. 110 000 Hidden Services

Licht und Schatten

Weil Hidden Services bewusst verborgen werden und fluktuieren, lassen sie sich kaum wissenschaftlich auswerten. Aufgrund solcher methodologischen Schwierigkeiten beschränken sich die meisten Untersuchungen auf Ausschnitte des Dark Webs zu bestimmten Zeitpunkten. Websites im Dark Web funktionieren mittlerweile so wie ihre WWW-Pendants. Es gibt Shops, Chats und Foren. Mangels effizienter Suchmaschinen dokumentieren zahlreiche Wikis, welche Dark-Web-Websites welche Adresse haben. Aber auch über Google lassen sich Adressen zu Dark-Web-Wikis finden. Nutzerkommentare und Bewertungen sind üblich. Einer britischen, nichtwissenschaftlichen Studie zufolge sind circa 50 Prozent der Dienste im Dark Web als legal einzustufen. Darunter fallen etwa

Foren, in denen Themen diskutiert werden, die in einigen Ländern tabuisiert sind. Auch Journalisten und Aktivisten nutzen das Dark Net aus Angst vor Verfolgung durch autoritäre Regierungen. Sichere Kommunikationsplattformen für Whistleblower (»Secure Drops«) werden im Dark Web auch von etablierten Organen wie der *Washington Post* gehostet. Tor wird insbesondere von Bürgern in repressiven Regimen genutzt, um die Internet-Zensur zu umgehen und auf westliche Dienste zugreifen zu können. Aus diesem Grund sponsert das US State Department seit 2011 die Entwicklung und Verbreitung von Tor im Rahmen der Internet Freedom Agenda.

Das Tor-Netzwerk wurde Mitte der 1990er Jahre am United States Naval Research Lab mit dem Ziel entwickelt, geheimdienstliche und militärische Kommunikation zu verbergen, und diese Funktion erfüllt es auch heute noch. Auch staatliche Cyber-Angriffe laufen über Tor.

Cyber-Kriminalität im Dark Net und Internet

Wie jede Technologie kann auch das Dark Web missbraucht werden. Die in den Medien oft zitierten illegalen Marktplätze (Cryptomarkets) für Waffen und Drogen machen jedoch nur einen sehr kleinen Teil der Websites im Dark Web aus (0,3 bzw. 4%) aus. Eine niederländische Studie kam 2016 zu dem Schluss, dass es rund 50 sogenannte Kryptomärkte gibt, auf denen Drogen und Waffen gehandelt werden. Einige davon haben Prominenz erlangt, wie etwa die 2013 geschlossene Plattform Silk Road.

Drogenhandel ist auf diesen Kryptomärkten das größte Phänomen im Bereich Cyber-Kriminalität. 57 Prozent der Angebote auf den 8 größten Märkten betreffen Drogen, wobei der Großteil auf Cannabis und Amphetamine entfällt. Harte Drogen wie Heroin werden dort selten gehandelt. Die Drogenmärkte verbuchen einen monatlichen Umsatz zwischen 10 und 18 Millionen Euro.

Malware und gestohlene digitale Güter sind neben Drogen und verschreibungspflichtigen Medikamenten eine häufige Produktkategorie auf Kryptomärkten. Die folgenden digitalen Güter waren 2018 auf einer Plattform namens Dream Market die meistgehandelten: kompromittierte Nutzeraccounts (42%), Kreditkartendetails (29%), einfache Hacking-Tools (10%), Ausweisdokumente (6,7%), komplexere Exploits (0,9%) und diverse Arten von Schadsoftware (je ca. 0,7%). Zudem gibt es eine rege Community bösartiger Hacker, die sich dort zum Erfahrungsaustausch treffen.

Auch der Vertrieb von Kinderpornografie findet über das Dark Web statt. Interessanterweise wird in diversen Kryptomärkten der Handel mit Kinderpornografie aber nicht toleriert und mit Ausschluss sanktioniert. Laut einer kürzlich erschienenen Studie gibt es nur etwa 51 dezidierte Seiten mit kinderpornografischen Inhalten im Dark Web. Gleichwohl muss man hier von einer höheren Dunkelziffer ausgehen.

Europol und die Europäische Beobachtungsstelle für Drogen und Drogensucht stellen in einer aktuellen Untersuchung fest, dass der Drogenhandel über Dark Nets verglichen mit dem Handel im offenen WWW relativ klein ist. Verglichen mit dem Offline-Drogenhandel spielt das Dark Net zwar eine wachsende, bisher aber dennoch eher marginale Rolle. Die Autoren einer Studie aus dem Jahr 2018 beleuchteten die Einnahmen aus dem Verkauf von Drogen auf den 8 größten Kryptomärkten im Dark Web. Demnach werden dort jährlich insgesamt rund 61 Millionen US-Dollar umgesetzt. Verglichen mit dem Gesamtvolumen des europäischen Drogenhandels (ca. 24–31 Mrd. Euro im Jahr), hat das Dark Net also einen Anteil von nur etwa 1 Prozent an diesem Geschäft. Laut einer Analyse des EU-Parlaments spielt das Dark Net auch für Formen der Cyber-Kriminalität (u. a. Software-Piraterie, Urheberrechtsverletzungen, digitaler Steuerbetrug, Kreditkartenbetrug und Click-Fraud) eine geringere Rolle als oft angenommen wird. Es trage nur zu circa 1 Prozent der direkten wirtschaftlichen Schäden bei, die durch diese Arten von Cyber-Kriminalität entstehen. Der weitaus größere Teil werde durch Cyber-Kriminali-

tät im regulären Internet verursacht, etwa durch digitale Steuervermeidung. Allerdings sind Sekundärschäden kaum zu berechnen.

Es gibt auch erheblich mehr kinderpornografische Angebote im frei verfügbaren Teil des Internets als im Dark Web. Eine Studie von 2014 kommt zu dem Schluss, dass von rund 31 000 mit Kinderpornografie assoziierten Websites nur 51, also 0,2 Prozent, über das Dark Net gehostet wurden. Der Rest wird häufig in Ländern mit schwacher Staatlichkeit im regulären Deep Web gehostet. Aber auch die direkte Distribution über Mailinglisten oder Messenger-Dienste ist weiter verbreitet als der Handel über das Dark Web.

Es gibt auch weitaus mehr Webshops für Narkotika im offenen Teil des Internets als im Dark Web. Drogenhandel findet zudem in viel stärkerem Maße über öffentliche Social Media Plattformen wie Facebook, Twitter und Reddit statt. Auch spezialisierte Apps und Messenger-Kommunikation spielen im heutigen Drogenvertrieb eine größere Rolle als das Dark Web.

Das Dark Web und das Tor-Netzwerk sind also durchaus ein treibender Faktor für Kriminalität, verglichen mit dem Rest des Internets aber ein unbedeutender. Eine Fokussierung auf das Dark Net als zentralen Schauplatz für Straftaten wäre Zeichen einer unangemessenen Gewichtung des Problems. Jedwede politischen Maßnahmen müssen umfassender gedacht werden. Ein Verbot des Dark Nets würde folglich kaum etwas am Phänomen der Cyber-Kriminalität ändern.

Ein oder viele Dark Nets verbieten?

Wenn pauschal über ein Verbot des Dark Nets gesprochen wird, stellt sich als Erstes die Frage, was genau eigentlich damit gemeint ist. Historisch betrachtet war vor der Erfindung des World Wide Web 1991 das gesamte Internet eine Art nicht-indexiertes, unsichtbares Dark Web. Die Erfinder des Internet-Vorläufers Arpanet bezeichneten bereits in den 1970er Jahren all jene Computernetzwerke, die vom Arpanet isoliert waren, als Dark Net. Was also zum Dark Net zählt, ist willkürlich und eine Definition ex negativo: Das Dark Net ist ein Teil des Internets, der nicht das WWW ist und bestimmte kryptografische Verfahren zur Gewährleistung von Anonymität umfasst. Das trifft aber auf Vieles zu, etwa auf Virtual Private Networks (VPN), auf den HTTPS-Datenverkehr oder auf verschlüsselte Foren im regulären WWW. Es gibt auch noch andere Dark Nets, etwa das anonyme Peer-to-peer-Netzwerk Freenet oder das Invisible Internet Project (I2P). Die Marktplatzplattform OpenBazaar zerlegt verborgene Websites in Teile und speichert diese dezentral über alle Nutzer hinweg. All diese individuellen Dark-Networks sind nicht eindeutig voneinander getrennt, da das TCP/IP-Protokoll sie in einem Netzwerk vereint. Das zeigt, dass ein pauschales Verbot des Dark Nets schnell zu einem Akt der Überregulierung mit Kollateraleffekten werden kann. Wer das Dark Net verbieten will, verbietet fast zwangsläufig legitime Inhalte mit.

Technische Implikationen eines Verbots

Ein nationaler Alleingang beim Verbot des oder eines Dark Nets wäre kaum realisierbar, da durch das Internet zahlreiche Alternativen frei verfügbar sind. Ein Verbot von Tor würde bedeuten, dass der Staat kontrollieren müsste, welche Software auf den Geräten seiner Bürger installiert ist. Das stellt selbst autoritäre Regime wie China und Russland, die verschlüsselten Internet-Diensten den Kampf angesagt haben, vor große Probleme. Russland gab 2015 ein mehrjähriges, millionenschweres Forschungsprojekt zur Deanonymisierung des Tor-Netzwerks erfolglos auf. Tor kann seine Datenverbindungen über Tarnprotokolle als Verkehr zu legitimen Websites maskieren und somit nicht mit klassischen Blacklisting-Internetfiltern zensiert werden. China ist nur deshalb in der Lage, den Tor-Datenverkehr zu blockieren, weil es alle Zugänge zum globalen Internet mit der »Great Firewall« überwacht und alle Pakete des Internetdatenverkehrs per Deep-Packet-Inspection nach Tor-Indikatoren durchsucht. Das

erfordert diverse Rechenzentren samt Supercomputern an zentralen Internet-Glasfaserleitungen. Die Durchsetzung eines Dark-Net-Verbots wäre also ohne eine gigantische Zensurinfrastruktur und ohne eine Segregation des deutschen Internets vom Rest der Welt kaum zu bewerkstelligen. Ein solches Vorhaben wäre weder mit wirtschaftlichen Interessen kompatibel noch mit demokratischen Normen.

Politische Konsequenzen einer Verbotspolitik

Das Verbot eines Dark Nets, zum Beispiel des Tor-Netzwerks, hätte international Signalwirkung. Mit einem solchen Schritt würde sich Deutschland einer Koalition autoritärer Regime wie Russland oder China anschließen. Diese fordern derartige Maßnahmen schon seit Jahren und sind bisher am Widerstand der liberalen westlichen Demokratien gescheitert. Mit der Entscheidung für ein Verbot würden die repressiven Tendenzen in der Internet-Governance gestärkt und würde zudem weltweit der Boden für Menschenrechtsverletzungen bereitet. Aus diesem Grund haben demokratische Regierungen ein solches Vorgehen bisher stets verhindert und Tor als Medium der freien Meinungsäußerung betrachtet.

Alternative Optionen

Ein alternativer Vorschlag wäre, die den Kryptomärkten zugrundeliegenden Technologien zu regulieren. Dazu gehören im Wesentlichen das Tor-Netzwerk (Browser, Hidden Services und physische Tor-Relay-Server) und die für das digitale Bezahlen eingeführten Kryptowährungen wie Bitcoin oder Monero. Die hinter all diesen Bausteinen steckende Technologie ist Verschlüsselung. Der Wesenskern von Verschlüsselung ist der Schutz der Integrität und Authentizität von Daten gegenüber unautorisierten Dritten, also auch staatlichen Stellen. Versuche, Verschlüsselungsverfahren zu verbieten oder mittels eingebauter Hintertüren staatlicher Kontrolle zu unterwerfen, sind bisher an technischen Realitäten gescheitert. Die Schwächung von Verschlüsselung würde die Cyber-Sicherheit im Zeitalter der Hacker und Cyber-Konflikte nachhaltig negativ beeinträchtigen, so dass der Weg des Verbots nicht ratsam ist.

Eine Möglichkeit wäre, dass das Betreiben von sogenannten Tor-Exit-Nodes, also Relays im Tor-Netzwerk, unter Strafe gestellt wird. Relay-Betreiber gerieten in der Vergangenheit immer wieder ins Visier von Strafverfolgungsbehörden. Ein Verbot des Betreibens von Exit-Nodes würde dazu führen, dass sich deutsche Tor-Nutzer über eines der rund 7000 ausländischen Tor-Relays verbinden würden, was die Internetverbindung lediglich verlangsamt. Das Tor-Projekt hat sich in der Vergangenheit als äußert resilient erwiesen, so dass bei Ausfall eines Exit-Nodes mit dem Nachwachsen neuer Relays zu rechnen ist. Dieser Weg wäre also wenig sinnvoll.

Zu guter Letzt gäbe es die Option, die Hidden Services selbst zu unterbinden. Die Politikwissenschaftler Daniel Moore und Thomas Rid sprechen sich etwa dafür aus, dass die Betreiber des Tor-Projekts die HS vom Tor-Netzwerk trennen sollten, da Erstere die legitimen Funktionen — also vor allem das anonyme Besuchen von Websites im Internet und die Umgehung von Zensurmaßnahmen — von Tor in Verruf bringen. Technisch betrachtet würde dies nur eine kleine Änderung im Protokoll der Tor-Infrastruktur erfordern. Damit würden verborgene HS unterbunden. Nicht-anonymisierte Tor-Seiten wie Secure Drops oder Facebook wären davon aber nicht betroffen. Im Wesentlichen würde sich der Schritt also gegen die Kryptomärkte richten. Einige der Pioniere des Tor-Projekts haben in der Vergangenheit immer mal wieder diese Option erwogen und auch in der Hacker-Community wird periodisch darüber diskutiert. Allerdings müsste sich dafür innerhalb dieser Community eine lautstarke Graswurzelbewegung formieren, damit die in Seattle ansässige Non-Profit-Organisation, die das Tor-Projekt verwaltet, umgestimmt werden

könnte. Die Hacker-Community könnte zudem selbst aktiv werden, indem die privaten Tor-Relay-Betreiber Anfragen für HS mittels einer von der Community kuratierten Blacklist blockieren. Viele Tor-Relays werden von Universitäten und NGOs betrieben, die hier vorangehen könnten. Im Einklang mit der kriminologischen Verdrängungstheorie ist aber davon auszugehen, dass Nutzer nach dem Wegfall der Tor-HS zu alternativen Technologien abwandern würden.

Neues IT-Sicherheitsgesetz

Im gegenwärtigen Entwurf des neuen IT-Sicherheitsgesetzes von 2019 soll »das Zugänglichmachen von Leistungen zur Begehung von Straftaten« strafbar gemacht werden. Die Klausel zur Änderung des Strafgesetzbuches § 126a ist besonders weit gefasst. »Wer Dritten eine internetbasierte Leistung zugänglich macht, deren Zweck oder Tätigkeit darauf ausgerichtet ist, die Begehung von rechtswidrigen Taten zu ermöglichen, zu fördern oder zu erleichtern, wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft.« Unter diese Bestimmung würde faktisch das gesamte TCP/IP-Internet fallen. Entgegen dem ursprünglichen Entwurf des Bundesrats ist die Klausel auch nicht mehr auf bestimmte, besonders schwere Delikttypen (Kinderpornografie) begrenzt. Je nach Rechtsprechung könnte damit auch das Betreiben von legitimen Tor-Nodes kriminalisiert werden. Eine engere gesetzliche Regelung, die sich auf bestimmte Straftaten sowie auf das konkrete administrative Betreiben von Dark-Web-Foren auf der Anwendungsebene, also das Dark Web, beschränken würde, wäre verhältnismäßiger. Problematisch ist eine weitgefasste Dark-Net-Klausel auch im Hinblick auf Entwicklungen, die sich bereits abzeichnen: Wenn in Zukunft mehr Dienste über Peer-to-peer-Services wie Blockchains gehostet werden, würde jeder Nutzer der Technologie — wissentlich oder unwissentlich — beim »Zugänglichmachen« von Kryptomärkten mitwirken. Verfassungsrechtler sehen eine Ausweitung kritisch, da Mittäter schon heute über eine Beihilfehandlung belangt werden können.

Polizeistreifen im Dark Net

Die zentrale politische Herausforderung liegt darin, die negativen Effekte des Dark Webs (Hidden Services und Kryptomärkte) einzudämmen und gleichzeitig die positiven Effekte des Dark Nets (Whistleblowing, Schutz vor Repression) zu bewahren. Dies lässt sich über ein pauschales Verbot oder die Strafbarmachung von Tor-Diensten nicht erreichen. Es ist nachvollziehbar, dass der Gesetzgeber Ermittlungen im Dark Net vereinfachen will. Dieses Ziel ließe sich aber durch eine verstärkte Präsenz und eine Verbesserung der Ausbildung und Ausstattung der Dark-Web-Fahnder leichter erreichen. Diese Maßnahmen würden nicht nur bei der Bekämpfung der Kriminalität im Dark Web helfen, sondern auch im Hinblick auf das reguläre Internet sinnvoll sein.

Traditionelle Strafverfolgung und neue Ermittlungsstrategien

Das Dark Web ist dem Internet ähnlicher als oft angenommen. Die Cyber-Sicherheit von Kryptomärkten und die IT-Sicherheitspraktiken vieler Nutzer sind nicht perfekt und somit anfällig für innovative Ermittlungsmethoden der Strafverfolgungsbehörden, inklusive staatliches Hacking. Oft ist nicht einmal der Einsatz von Schadsoftware (z. B. Bundestrojaner) erforderlich, sondern reicht der clevere Einsatz von frei verfügbaren Tools aus.

Wie im regulären Internet sind auch im Dark Web die Nutzer faul und verwenden über viele Websites hinweg die gleichen Nicknames, E-Mail-Adressen und schwache Passwörter. Kryptomärkte sind oft unsicher konfiguriert und damit für intelligente Strafverfolgungsoperationen angreifbar. Die FBI-Operation gegen den Kryptomarkt Silk Road machte sich etwa einen Fehler in der Anmeldemaske des Marktes zunutze, dank dessen User deanonymisiert werden konnten. Nutzer und Betreiber verwenden für

Dark-Web-Foren oder Bitcoin-Wallets oft die gleichen E-Mail-Adressen, die sie auch im regulären Internet nutzen. Das macht sie über verschiedene Internet-Dienste hinweg verfolg- und identifizierbar. Bei der erfolgreichen Strafverfolgungsoperation Bayonet, in deren Rahmen es gelang, zwei der größten Kryptomärkte zu deaktivieren und deren Infrastruktur zu beschlagnahmen, nutzten die Ermittler diesen Umstand aus. In einer international koordinierten Aktion übernahm das FBI die Kontrolle über den Kryptomarkt Alphabay. Als dies bekannt wurde, wanderten die Nutzer in den von Europol fast zeitgleich übernommenen Kryptomarkt Hansa ab. Dabei verwendeten sie oft die gleichen Namen und Passwörter und konnten so identifiziert werden.

Die Betreiber von Online-Märkten treten zudem oft unvorsichtig im regulären Internet in Erscheinung, wie etwa in den Foren Reddit oder 4chan. Sie verwenden für ihre Shops zudem häufig Vorschaubilder von anderen Websites wieder, was sie identifizierbar macht. Oft entfernen sie die EXIF-Metadaten aus Bilddateien nicht. All diese Indizien können auch ohne Hacking durch sorgfältige Polizeiarbeit gesammelt und zu Beweismaterial verdichtet werden. Bitcoin-Transaktionen können durch sogenannte Chain-Analysis und Big-Data-Verfahren auch heute schon zum Teil deanonymisiert werden. Das zeigt, dass sich Dark-Web-Ermittlungen nicht nur auf das Dark Net beschränken dürfen, sondern holistisch verschiedene Informationen und Quellen im offenen Internet miteinbeziehen müssen (Open Source Intelligence). Erforderlich ist dazu allerdings eine permanente Präsenz der Polizei im Dark Web bzw. eine kontinuierliche Aktualisierung des Lagebilds.

Der ehemalige Direktor des US-Heimatschutzministeriums Michael Chertoff weist darauf hin, dass die Anonymität im Dark Net für Strafverfolgungsbehörden nicht nur ein Nachteil, sondern auch ein Vorteil ist: Für Website-Betreiber und Nutzer ist nicht ohne weiteres nachvollziehbar, ob das Gegenüber nicht ein Undercover-Polizist ist bzw. der Kryptomarkt nicht von der Polizei gehostet wird. Viele erfolgreiche Strafverfolgungsoperationen gegen solche Märkte machen sich genau diesen Umstand zunutze. Interessant ist in diesem Zusammenhang die FBI-Operation Pacifier: durch einen technischen Hack gelang es dem FBI, die Kontrolle über die Kinderpornografie-Seite Playpen zu übernehmen und so die Nutzer zu deanonymisieren. Bei der Operation Bayonet gegen den Kryptomarkt Hansa konnten Ermittler den Markt-Server in einem Rechenzentrum lokalisieren und vor Ort den Software-Code des HS manipulieren. Die Kontrolle des HS-Servers ist immer das primäre Ziel, da auf diese Weise alle Transaktionen verfolgt und Nutzerdaten trotz Anonymisierung extrahiert werden können. Ferner können sogenannte »beacon files« in illegale Güter, wie etwa pornografische Bilder, implantiert werden, die den Ermittlern die wahre IP-Adresse eines Downloads mitteilen. Wenn Nutzer in Kryptomärkten, die von der Polizei kontrolliert werden, physische Waren bestellen, können Sendungen nachverfolgt werden (etwa durch GPS-Sender in Paketen). Packstationen — die von den Kunden bevorzugten Zustellorte für illegale Warensendungen — können videoüberwacht und die Empfänger bei Abholung festgenommen werden.

Zwar ist die physische Lokalisierung und Übernahme von HS-Servern komplex, zeitaufwendig und kostenintensiv, sie ist aber enorm effektiv. Bei der Operation gegen Hansa konnten durch die Übernahme des Servers mehr als 400 000 Nutzer identifiziert und über 10 000 physische Privatadressen ermittelt werden. Bessere Ermittlungstechniken tragen dazu bei, dass die durchschnittliche Lebenszeit eines Kryptomarkts bei nur etwa 12 Monaten liegt. Allerdings zieht das Abschalten eines Dienstes in der Regel binnen Sekunden das Auftauchen neuer, alternativer Plattformen nach sich.

Polizeiausbildung und internationale Zusammenarbeit

Europol hat in einer kürzlich erschienenen Studie dargestellt, dass in den verschiedenen europäischen Polizeibehörden zum Teil noch erhebliche Wissenslücken bezüglich

des Dark Nets existieren. Ein häufiger Fehlschluss ist etwa anzunehmen, dass das traditionelle kriminalistische Erfahrungswissen im Angesicht der neuen Kriminalitätsformen, die das Dark Net ermöglicht, obsolet geworden ist. Die digitale Ermittlungsarbeit gleicht in einigen Bereichen sehr stark den bewährten Praktiken des Analysierens und Verbindens von verschiedenen Spuren. Das Ziel sollte daher sein, die in Europa durchaus vorhandene Expertise in Sachen Dark-Net-Ermittlungen besser zu bündeln und zu teilen.

Elementar wäre es dabei, mehr Polizeibeamte in neuen technischen Verfahren und Kenntnissen der IT-Sicherheit auszubilden und diese Fähigkeiten mit den bekannten und erprobten Ermittlungsmethoden zu verknüpfen. Nur die Kombination dieser Skill-Sets wird langfristig zum Erfolg führen. Europol hat dafür spezielle Teams aufgestellt, die IT-Security-Experten, IT-Juristen und erfahrene Kriminalisten mit verschiedenen Spezialgebieten zusammenbringen. Solche Dark Net Task Forces sollten gestärkt und auch in den Mitgliedstaaten auf- und ausgebaut werden. Das bedeutet, dass die EU und die Mitgliedstaaten in diesen Bereichen »capacity building« betreiben müssen.

Eine rege internationale Kooperation ist bei der Bekämpfung von Kryptomärkten, die oft über mehrere Ländergrenzen hinweg gehostet werden, zentral. Operationen gegen solche Märkte können nur dann erfolgreich sein, wenn zeitgleich mehrere der wichtigsten Server von Strafverfolgungsbehörden übernommen werden. Die Ermittlungen sollten also, ähnlich wie bei der gemeinsamen Terrorbekämpfung, europäisch koordiniert werden. Dazu gehört ganz wesentlich, dass die EU-Partner elektronische Beweismittel reibungsloser austauschen und sich gegenseitig schneller Rechtshilfe leisten.

Auch die Zoll-Behörden sollten verstärkt und die Kooperation unter ihnen intensiviert werden. Ein Großteil der über das Dark Net verschickten physischen Waren wandert unkontrolliert über die offenen EU-Binnengrenzen. Deshalb wäre ein internationaler Austausch darüber, welche Methoden Kryptomarkt-Händler nutzen, damit ihre Päckchen vom Zoll nicht erkannt werden, elementar. Finnland beispielsweise hat vergleichsweise strenge Paketkontrollbestimmungen, weshalb Kryptomarkt-Anbieter aus Angst vor Strafverfolgung weniger häufig Waren dorthin versenden. Zudem ist zu überlegen, ob man nicht maschinelles Lernen oder automatisierte Screening-Prozesse im Warenverkehr einführen sollte, zumindest bei Paketen, die an Packstationen geliefert werden. Hier wäre die EU gefragt, einen Entwurf zu präsentieren, der die bestehenden Freiheiten wie das Postgeheimnis nicht unnötig einschränkt, aber bestimmte Kontrollen ermöglicht.

Fazit

Das Dark Net ist Schauplatz durchaus abscheulicher Kriminalitätsformen, die nicht zu verharmlosen sind. Eine sachliche Betrachtung zeigt aber, dass die gleichen Straftaten in oft größerem Ausmaß im allgemeinen Internet oder in der physischen Welt stattfinden. Eine zu enge Fokussierung auf das Dark Net als Brennpunkt der Kriminalität ist daher wenig sinnvoll. Neue Ermittlungsmethoden haben schon gezeigt, dass die Anonymität von Straftätern im Dark Net kein unüberwindbares Hindernis mehr ist. Allerdings gleicht der Kampf gegen die Kriminalität im Dark Web einem stetigen Katz-und-Maus-Spiel. Auch die Kriminellen verwenden immer neue Methoden und die Polizei muss darauf reagieren. Damit sie dazu in der Lage ist, müssen innerhalb der EU mehr finanzielle Mittel für Personal, Ausbildung und Kooperation bereitgestellt und mehr Beamte in Verfahren der digitalen Technik geschult werden. Dieser Weg ist zwar kostenintensiver, aber auch nachhaltiger als scheinbar schnelle Lösungen in Form von Verboten oder einer Überregulierung, die technisch und politisch kaum ohne Kollateralschäden umsetzbar wären.

Dr. Matthias Schulze ist Wissenschaftler in der Forschungsgruppe Sicherheitspolitik.

SWP
Stiftung Wissenschaft und Politik
Deutsches Institut für Internationale Politik und Sicherheit

Ludwigkirchplatz 3—4
10719 Berlin
Telefon +49 30 880 07-0
Fax +49 30 880 07-100
www.swp-berlin.org
swp@swp-berlin.org

ISSN 1611-6364
doi: 10.18449/2019A28